УДК 004.77

М. С. Мамута[1], І. В. Кравченко[1], О. Д. Мамута[2]

СПОСОБИ З'ЄДНАННЯ З ВІРТУАЛЬНИМ СЕРВЕРОМ AWS, ЩО РОЗТАШОВАНИЙ В ПРИВАТНІЙ ПІДМЕРЕЖІ

[1]Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ

[2]Інститут фізики Національної Академії наук України, Київ

Анотація. В сучасному світі всеохоплюючої діджиталізації гостро стоїть питання кібербезпеки і безпечної роботи з даними в кіберпросторі. На сьогоднішній день це питання особливо гостро постає для України, де кількість та потужність кібератак зросла в кілька разів за останній рік. Особливо вразливим стає бізнес, який працює з приватними даними клієнтів. Звичайно ж, ідеальним варіантом є розміщення таких даних на серверах, які не мають виходу в інтернет. Але з огляду на загальносвітову тенденцію переміщення в хмару, це є неможливим і для бізнесових, і для приватних даних. А отже постає питання захисту приватних даних в хмарі. З цією метою постачальники хмарних послуг пропонують сервіси для створення приватних підмереж без доступу до інтернету. Тож стає актуальним питання як безпечно здійснити доступ до даних в таких підмережах.

Одним із провідних вендорів хмарних послуг є Амазон з платформою Amazon Web Services. Амазон пропонує сервіс Virtual Private Cloud для налаштування віртуальної мережі. В роботі проаналізовано особливості налаштувань при створенні підмереж з доступом до інтернету та без доступу до інтернету. Проаналізовано спосіб з'єднання з віртуальним сервером за мережевим протоколом Secure Shell. Проаналізовані недоліки такого способу. Запропоновано використовувати сервіс Амазону Systems Manager, що надає можливість безпечного доступу до даних без створення зайвих ресурсів по захищеному каналу між Systems Manager Agent та центром обробки даних Амазону, є економічно вигідним і зручним. Розглянуто особливості налаштувань політик доступу до віртуальних серверів при використанні сервісу Systems Manager. Розглянуто налаштування точок доступу до приватної мережі для здійснення з'єднання Systems Manager з віртуальним сервером, який немає публічної IP адреси та виходу в інтернет.

Ключові слова: AWS, Bastion Host, SSH, приватна підмережа, endpoint, Systems Manager.

Abstract. In today's world of total digitization cyber security and safe work with data in cyberspace are the most important questions. Especially this is actual for Ukraine, where the number and power of cyberattacks has increased several times over the last year. Businesses that work with private customer data become especially vulnerable. Of course, the ideal option is to place such data on servers that don't have Internet access. But according to the global trend of moving to the cloud, it is inevitable for private data as well. And so, there is a question of protecting private data in the cloud. To this end, cloud service providers offer services to create private subnets without Internet access. Therefore, the question of how to securely access data in such subnets become actual.

One of the leader's vendors in cloud servicing is Amazon with its Web Services. Amazon offers a Virtual Private Cloud service for setting up a virtual network. The article deals with the analysis of configuration features at the stage of creation of subnets with and without Internet access. The method of connection to a virtual server, located in a private subnet, using the Secure Shell network protocol was analyzed. However, this method has a number of disadvantages. It requires to launch an additional server and its administration. The method also has quite complex settings of the network and requires managing keys. Therefore, another method of connection to private EC2 instance was proposed. The method requires Amazon Systems Manager service, which provides secure access to data without creating additional server, is cost-effective and convenient. At the same time, all connections take place over a secure channel between the Systems Manager agent and the Amazon data center. Main setting's features for the proposed method were considered.

Key words: AWS, Bastion Host, SSH, private subnet, endpoint, Systems Manager.

DOI: https://doi.org/10.31649/1999-9941-2023-57-2-33-42.

Вступ

На сьогоднішній день для України гостро постають питання надійного зберігання даних, забезпечення безперервного доступу та безпеки в кіберпросторі. Організації як приватного, так і державного сектору здійснюють переміщення в хмару та розміщують найбільш вразливі дані в приватних підмережах без доступу до інтернету. В «хмарному світі» для створення та адміністрування таких мереж зручним є використання технології Virtual Private Network, а постачальники хмарних послуг [1] пропонують власні сервіси для її реалізації. Тому важливим питанням є дослідження особливостей налаштування віртуальних мереж та способів безпечного доступу до приватних даних, що пропонують провідні вендори, зокрема Amazon Web Services (AWS).

AWS пропонує сервіс Virtual Private Cloud (VPC) для створення віртуальних мереж [2], який дозволяє повністю адмініструвати мережу, в тому числі обирати власний діапазон IP адрес, створювати підмережі, налаштовувати маршрутизацію та мережеві шлюзи.

З'єднання з віртуальним сервером зазвичай здійснюється за мережевим протоколом Secure Shell (SSH). Технологія SSH з'єднання полягає в тому, що доступ користувача, який під'єднаний до мережі інтернет, до хмарного віртуального серверу AWS (EC2 instance), що знаходиться в приватній підмережі, яка немає виходу в інтернет, проводиться не власними програмними засобами користувача, а засобами додаткового сервера AWS, який називають Bastion Host. Такий сервер розташовують в публічній підмережі, що має вихід в інтернет, та надають йому доступ до приватної мережі. Зовнішній користувач немає прямого доступу до віртуального сервера. Таким чином, щоб здійснити SSH з'єднання з віртуальним

сервером, що розташований в приватній підмережі, потрібно спершу користувачу здійснити з'єднання з Bastion Host, а вже з Bastion Host підключитись до потрібного серверу. З одного Bastion Host можна реалізувати доступ до кількох серверів в приватній підмережі.

Актуальність

Базові положення технології Virtual Private Network та кібербезпеки в приватних віртуальних мережах розглянуто в [3], в [4] описано хід трафіку від користувача через сервер-шлюз до приватної мережі. Проте потребують уточнення особливості налаштувань віртуальної мережі, та представляють інтерес альтернативні способи з'єднання з віртуальним сервером (без використання серверів-шлюзів).

Мета

Метою даної роботи є надання потенційним користувачам хмар засобів, які зменшують витрати та можливі помилки в створенні віртуальної мережі, встановленні SSH з'єднання з віртуальним сервером в приватній підмережі через сервери-шлюзи та за допомогою сервісу AWS Systems Manager.

Задачі

1. Дослідження можливостей та особливостей сервісів AWS та розробка типового алгоритму дій для з'єднання з віртуальним сервером.
2. Виявлення особливостей налаштувань віртуальних серверів, підмереж, протоколів з'єднання та знаходження оптимальних параметрів безпечного з'єднання за протоколом SSH на кожному етапі дій.

Розв'язання задач

Типовим порядком встановлення SSH з'єднання з віртуальним сервером, що розташований в приватній підмережі, чкерез сервери-шлюзи можна вважати наступні етапи:

1. Створення віртуальної мережі.
2. Створення та налаштування підмереж.
3. Запуск віртуальних серверів.
4. Встановлення з'єднання за мережевим протоколом Secure Shell.

Створення віртуальної мережі.

Створення віртуальної мережі VPC (Virtual Private Cloud) активується кнопкою Create VPC (рис. 1а) консолі AWS. У вікні створення віртуальної мережі (рис. 1б) слід зазначити назву мережі та вказати адресу безкласової адресації – IPv4 CIDR (Classless Inter-Domain Routing).

Оскільки VPC – це приватний ресурс, то дозволені лише адреси IPv4 з приватного діапазону за правилами Адміністрації адресного простору Інтернет (Internet Assigned Numbers Authority) [5]:

- ✓ 10.0.0.0 – 10.255.255.255 (в AWS записується наступним чином 10.0.0.0/8);
- ✓ 172.16.0.0 – 172.31.255.255 (в AWS записується наступним чином 172.16.0.0/12);
- ✓ 192.168.0.0 – 192.168.255.255 (в AWS записується наступним чином 192.168.0.0/16).

Діапазон обирається будь-який всередині наведених вище, головне, щоб VPC CIDR не перетинався з іншими, вже створеними власними мережами/підмережами (не було накладання діапазонів).

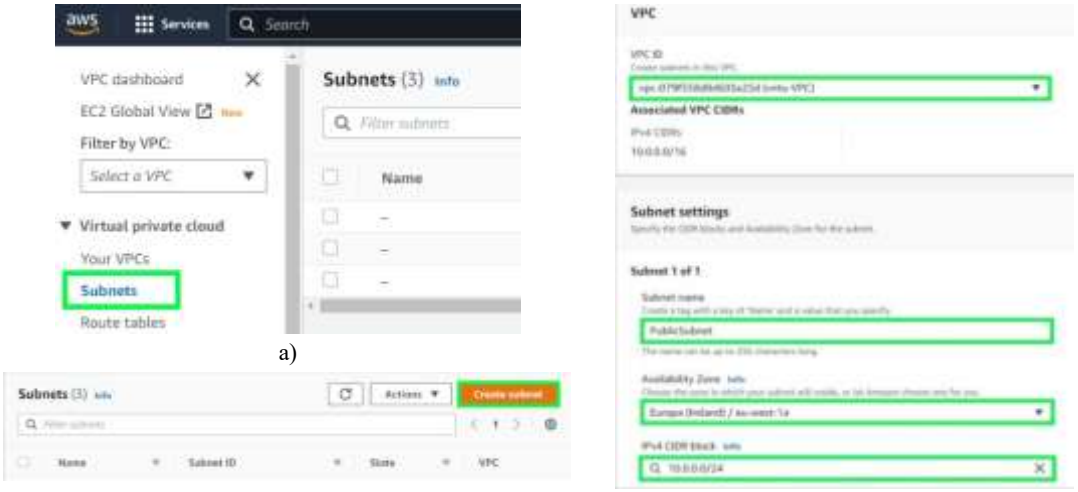
а) б)

Рисунок 1 – Створення віртуальної мережі: а) – панель консолі AWS; б) – поля сторінки створення VPC

Створення та налаштування підмереж.

Для переходу до підмереж потрібно в головному меню консолі AWS VPC обрати пункт **Subnets** (рис. 2а). Створення підмережі активується кнопкою **Create subnet** (рис. 2б) консолі AWS. У вікні створення підмережі обирається створена VPC, вказується назва підмережі, зона доступності (Availability Zone) та IPv4 CIDR block.

Для того, щоб публічна мережа мала вихід в інтернет потрібно налаштувати мережевий шлюз [6], маршрутизацію та увімкнути можливість автоматичного присвоєння IP адреси.



а) б) в)

Рисунок 2 – Створення підмережі: а) – головне меню консолі; б) – панель консолі; в) – поля сторінки створення subnet

Для роботи з мережевим шлюзом потрібно в головному меню консолі AWS VPC обрати пункт **Internet gateways** (рис. 3а). Створення мережевого шлюзу активується кнопкою **Create internet gateway** (рис. 3б) консолі AWS. У вікні створення мережевого шлюзу потрібно ввести його назву (рис. 3в).

а) б) в)

Рисунок 3 – Створення мережевого шлюзу: а) – головне меню консолі; б) – панель консолі; в) – поля сторінки створення internet gateway

Щойно створений мережевий шлюз має статус Detached (рис. 4а), і його потрібно приєднати до віртуальної мережі. Активується приєднання командою Attach to VPC з випадаючого списку Actions (рис. 4б). У вікні Attach to VPC (рис. 4в) зі списку доступних Available VPC обирається віртуальна мережа.

а) б) в)

Рисунок 4 – Приєднання мережевого шлюзу до віртуальної мережі: а) – панель консолі AWS; б) – активація приєднання; в) – поля сторінки приєднання

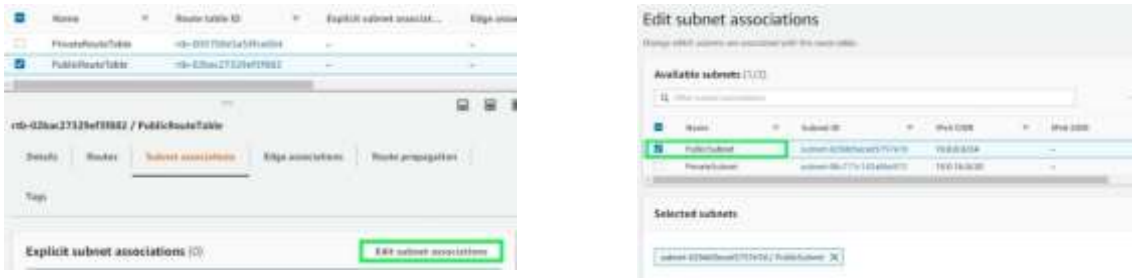
Тільки створення мережевого шлюзу недостатньо. Для забезпечення доступу з інтернету, потрібно ще налаштувати маршрутизацію [7].

Для роботи з маршрутизатором (Route tables) потрібно в головному меню консолі AWS VPC обрати пункт Route tables (рис. 5а). Створення маршрутизатора активується кнопкою **Create route table** (рис 5б) консолі AWS. У вікні створення потрібно вказати назву та обрати мережу (рис. 5в).

а) б) в)

Рисунок 5 – Створення маршрутизатора: а) – головне меню консолі; б) – панель консолі; в) – поля сторінки створення route table

Маршрутизатори для публічної та приватної підмережі створюються окремо. Після створення слід приєднати маршрутизатор до підмережі. Приєднання маршрутизатора активується кнопкою **Edit subnet associations** вкладки Subnet associations для обраної підмережі (рис. 6а). У вікні приєднання обирається потрібна підмережа (рис. 6б).



а) б)

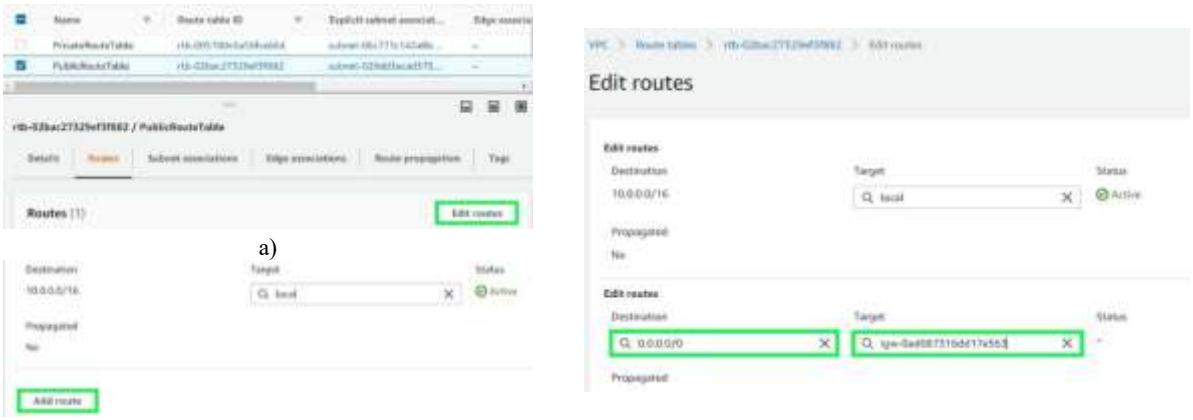
Рисунок 6 – Приєднання маршрутизатора: а) – список підмереж; б) – вікно приєднання

Потоками трафіка в віртуальній мережі управляють правила (Routes). За замовчуванням при створенні мережі прописується правило, яке дозволяє проходження трафіку локально, в межах IPv4 CIDR block створеної мережі. Для публічної підмережі потрібно додатково прописати правила для виходу в інтернет. Додавання правил активується кнопкою **Edit routes** вкладки Routes для обраної підмережі (рис. 7а). У вікні додавання правил створення нового правила активується кнопкою **Add route** (рис. 7б). У відкритому вікні Edit routes вказується адреса CIDR block для всіх IP адрес та куди направляється трафік (рис. 7в). Трафік для виходу в інтернет направляється в мережевий шлюз. Додане правило направляє трафік в мережевий шлюз для всіх IP адрес, які не входять в IPv4 CIDR block приватної мережі

Автоматичне присвоєння IP адреси активується кнопкою **Actions** командою Edit subnet settings (рис. 8а) випадаючого списку в консолі AWS для обраної підмережі. У вікні налаштувань підмережі обирається опція Auto-assign IP settings (рис. 8б).

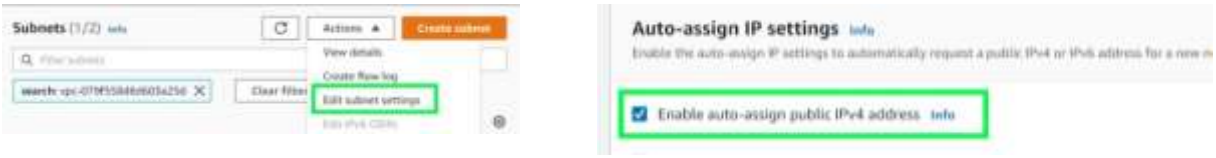
Запуск віртуальних серверів.

Для запуску віртуального серверу потрібно обрати сервіс Elastic Compute Cloud (EC2). Активується запуск кнопкою **Launch instances** (рис. 9а) консолі AWS. Принциповими для обох серверів є проведення налаштування мережі, які активуються кнопкою **Edit** групи налаштувань Network settings (рис. 9б). У вікні налаштувань обирається власна VPC, вказується підмережа, де буде розміщено віртуальний сервер. Для Bastion Host перевіряється опція автоматичного присвоєння публічної IP адреси (рис. 9в), а для віртуального серверу в приватній підмережі – відсутність публічної IP адреси.



а) б) в)

Рисунок 7 – Додаванна правил для маршрутизатора: а) – панель консолі; б) – активація додавання правил; в) – поля сторінки додавання правил



а) б)

Рисунок 8 – Активація автоматичного присвоєння IP адреси: а) – панель консолі AWS; б) – поля сторінки автоматичного присвоєння IP адреси

а) б) в)

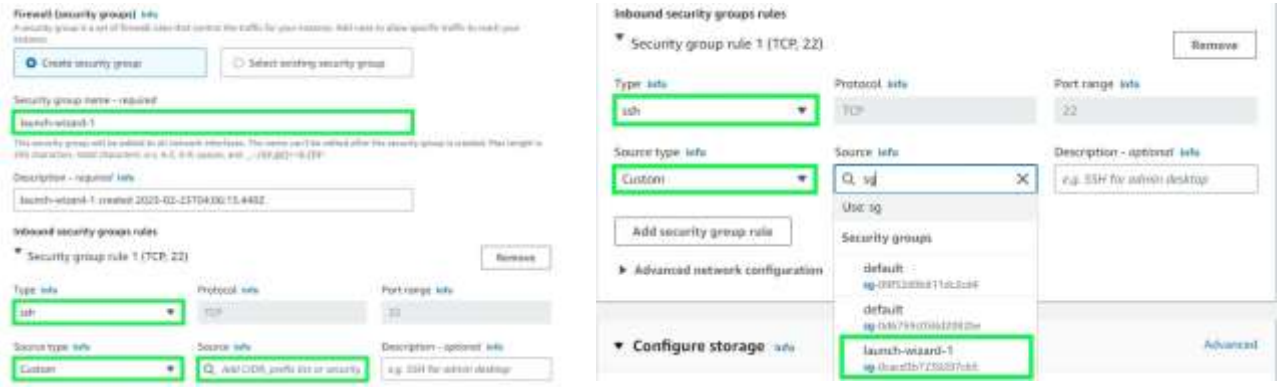
Рисунок 9 – Запуск віртуального серверу: а) – панель консолі AWS; б) – поля сторінки запуску віртуального сервера; в) поля сторінки налаштувань мережі

Особливу важливість представляють налаштування групи безпеки (security group). Security group – це своєрідний firewall, який контролює відкриття портів та список IP адрес, з яких доступне з’єднання з віртуальним сервером. Потрібно створити власну security group, дати їй назву (або скористатись назвою, яку пропонує AWS за замовчуванням), відкрити порт 22 для можливості встановлення SSH з’єднання та обмежити список IP адрес, з яких дозволено з’єднання з віртуальним сервером. Рекомендується для віртуального серверу Bastion Host дозволити доступ лише для public CIDR організації або взагалі однієї IP адреси (рис. 10а), а для віртуального серверу, що розташований в приватній підмережі, обов’язково дозволити доступ лише з Bastion Host, обравши відповідну йому групу безпеки (рис. 10б).

Встановлення з’єднання за мережевим протоколом Secure Shell.

Встановлення SSH з’єднання з віртуальними серверами здійснюється одним із способів, описаних в [8]. Для авторизованих користувачів найбільш зручним є використання вбудованої опції AWS – EC2 instance connect. Проте при обмеженні списку IP адрес даний спосіб потребує додаткових налаштувань. Для спрощення рекомендується використовувати Windows PowerShell (рис. 11а).

Особливістю здійснення SSH з'єднання з віртуальним сервером, що розташований в приватній підмережі, є те, що файл з ключем розташований на клієнтському ПК, а з’єднання здійснюється через Bastion Host, тому ключ потрібно розмістити там. При цьому слід обмежити права доступу до ключа. Також потрібно врахувати Amazon Machine Image віртуального сервера, від цього залежить ім’я користувача за замовчуванням [9].



а) б)

Рисунок 10 – Налаштування групи безпеки: а) – для Bastion Host; б) – для віртуального сервера, що розміщений в приватній підмережі

Питання розміщення ключа на Bastion Host можна вирішити за допомогою редактора «vi» [10]. Для цього потрібно в Bastion Host створити файл з назвою ідентичною назві приватного ключа на клієнтському ПК, вставити повністю зміст файлу приватного ключа в щойно створений файл та зберегти зміни.

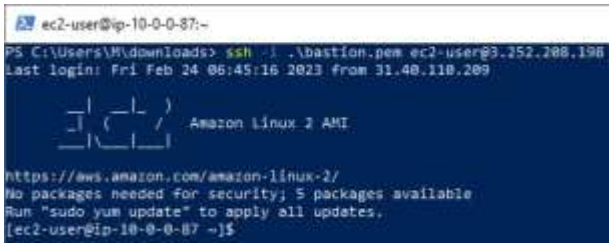
Далі потрібно захистити створений файл шляхом обмеження прав доступу. Надається лише право читання і лише для власника. Для цього прописується в PowerShell [9]:

chmod 400 назва ключа.pem

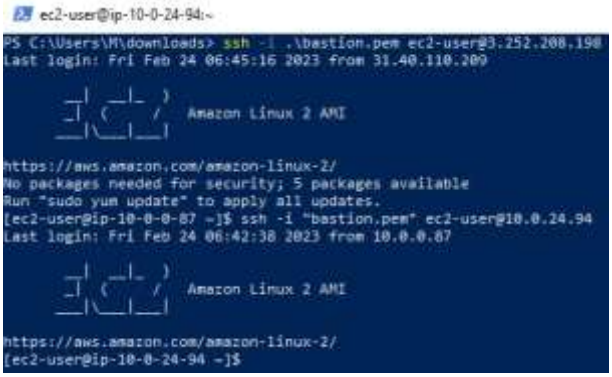
Після налаштувань ключа в командному рядку здійснюється SSH з'єднання з віртуальним сервером, що розташований в приватній підмережі (рис. 11б):

ssh -i “bastion.pem” ec2-user@ 10.0.24.94,

де bastion.pem – ім’я файлу приватного ключа, що знаходиться на Bastion Host, 10.0.24.94 – приватна IP адреса віртуального сервера, що розташований в приватній підмережі.



а)



б)

Рисунок 11 – SSH з’єднання з віртуальними серверами: а) – з Bastion Host; б) – з віртуальним сервером, що розміщений в приватній підмережі

Таким чином, SSH з’єднання з віртуальним сервером, що розташований в приватній підмережі, потребує:

- ✓ запуск додаткового сервера (Bastion Host) та його адміністрування;
- ✓ ретельне налаштування власне самої мережі та підмереж, що складається з: налаштування маршрутизації та мережевого шлюзу, відкриття портів, обмеження трафіку за допомогою груп безпеки, контроль присвоєння IP адрес;
- ✓ адміністрування приватних ключів.

Для спрощення з’єднання з віртуальним сервером доцільно використовувати сервіс AWS Systems Manager [11]. Даний сервіс дає можливість керувати віртуальним сервером завдяки спеціальному програмному забезпеченню – AWS Systems Manager Agent (SSM Agent) [12].

SSM Agent автоматично встановлюється на віртуальному сервері та зв’язується з сервісом AWS Systems Manager Session Manager [13]. А отже користувач може заходити в віртуальний сервер за допомогою сервісу AWS Systems Manager Session Manager та передавати певні команди. Крім того, «логи» з’єднання можна зберігати в S3 або CloudWatch Logs.

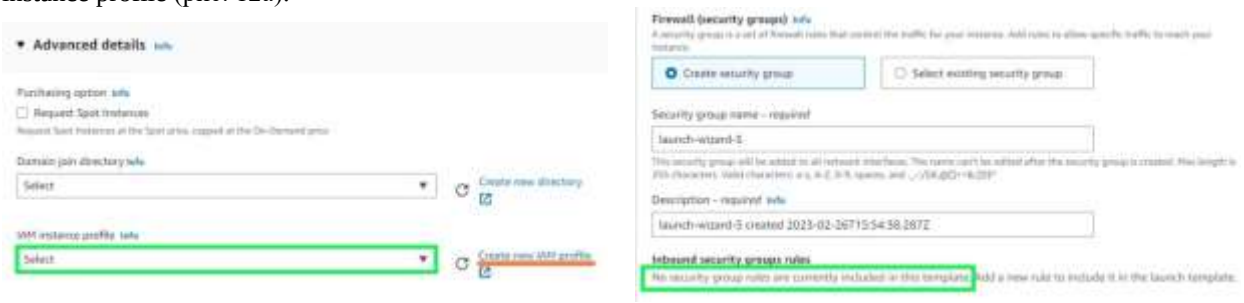
В зв’язку з тим, що віртуальний сервер приватної підмережі не має публічної IP адреси та доступу з інтернету, потрібні додаткові налаштування, а саме: створення точок доступу до приватної мережі – VPC endpoint для AWS Systems Manager [14].

Отже, з’єднання з віртуальним сервером, що розташований в приватній підмережі, за допомогою Session Manager складається з наступних етапів:

1. Запуск віртуального сервера з необхідними налаштуваннями.
2. Налаштування VPC endpoints.
3. Власне з’єднання.

Запуск віртуального сервера з необхідними налаштуваннями.

При запуску віртуального сервера ключовим моментом є надання йому дозволу зв’язуватись із сервісом AWS Systems Manager. З цією метою в розширених налаштуваннях потрібно створити та під’єднати до віртуального сервера профіль керування доступом – IAM (Identity and Access Management) instance profile (рис. 12а).



а) б)

Рисунок 12 – Налаштування віртуального сервера: а) – налаштування мережі; б) розширені налаштування

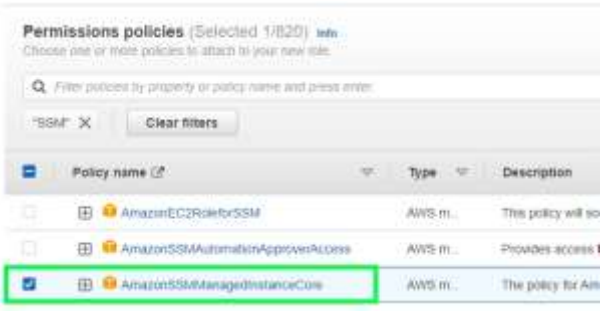
Створюється IAM instance profile за допомогою сервісу AWS Identity and Access Management (IAM) [15]. Активується створення профілю кнопкою Create new IAM profile в групі розширених налаштувань сторінки запуску віртуальної машини (рис. 12а). В новому вікні відкривається консоль AWS IAM.

Активується створення ролі для профілю кнопкою Create role (рис. 13а) консолі AWS. У вікні створення ролі слід обрати AWS service, а саме – EC2 (рис. 13б), далі потрібно обрати політику – AmazonSSMManagedInstanceCore (рис. 13в) та дати назву ролі.

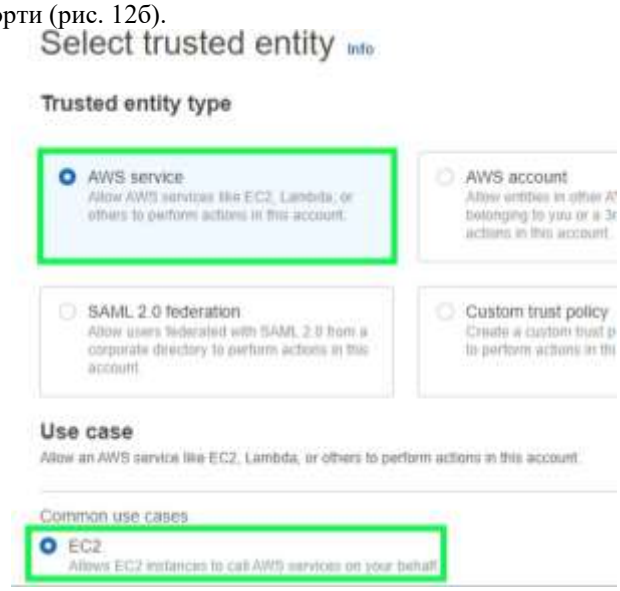
Крім того, рекомендуємо змінити наступні налаштування:

- ✓ пару ключів не варто створювати, в даному випадку вони не потрібні;
- ✓ в налаштуваннях мережі можна закрити всі порти (рис. 12б).

а)



в)



б)

Рисунок 13 – Створення ролі: а) – панель консолі AWS; б) – поля сторінки створення ролі; в) – політика доступу

Налаштування VPC endpoints.

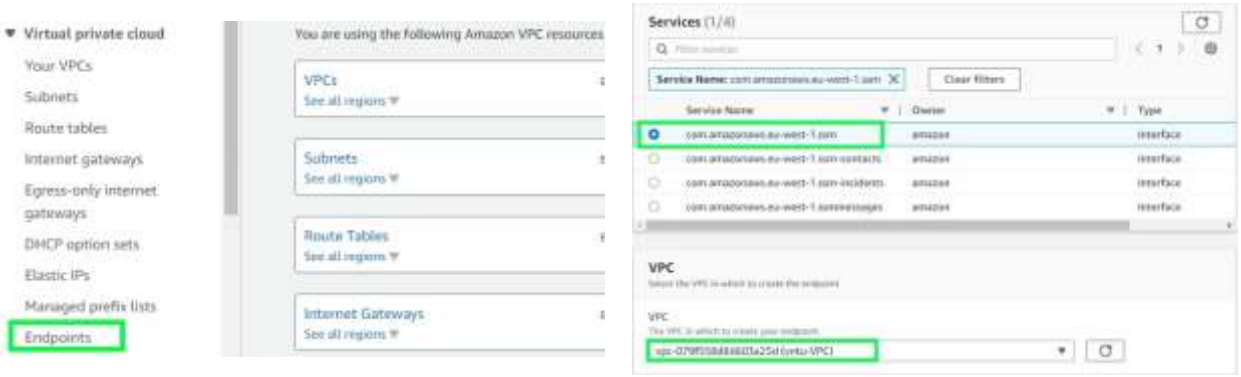
Для роботи з точками доступу потрібно в головному меню консолі AWS VPC обрати пункт Endpoints (рис. 14а).

У вікні створення endpoint потрібно здійснити ряд налаштувань:

- ✓ в групі Services обрати назву сервісу – com.amazonaws.eu-west-1.ssm (рис. 14б), де eu-west-1 – регіон, в якому розміщений віртуальний сервер;
- ✓ в групі VPC обрати свою мережу (рис. 14б);
- ✓ в групі Subnets обрати приватну підмережу та тип IPадреси, тобто IPv4;
- ✓ в Security groups обрати групу безпеки, яка буде приєднана до endpoint, в даній групі має бути дозволений inbound трафік через порт 443 за протоколом https.

Аналогічно потрібно створити ще дві endpoint – com.amazonaws.eu-west-1.ssmmessages та com.amazonaws.eu-west-1.ec2messages.

Вказані endpoints необхідні для реєстрації приватного серверу в Systems Manager, створення каналу зв'язку із Session Manager та надсилання/отримання команд.

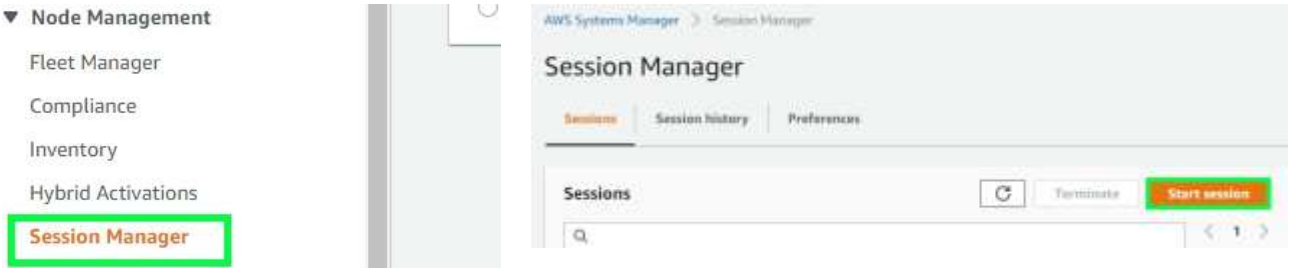


а) б)

Рисунок 14 – Консоль AWS VPC: а) – Endpoints; б) – налаштування на сторінці створення endpoint

Встановлення з'єднання за допомогою сервісу AWS Systems Manager.

Встановлення з'єднання проводиться на сторінці Session Manager. Сторінка відкривається пунктом Session Manager головного меню консолі AWS Systems Manager (рис. 15а). Активується процедура встановлення з'єднання на сторінці Session Manager кнопкою Start Session консолі AWS Systems Manager (рис. 15б).



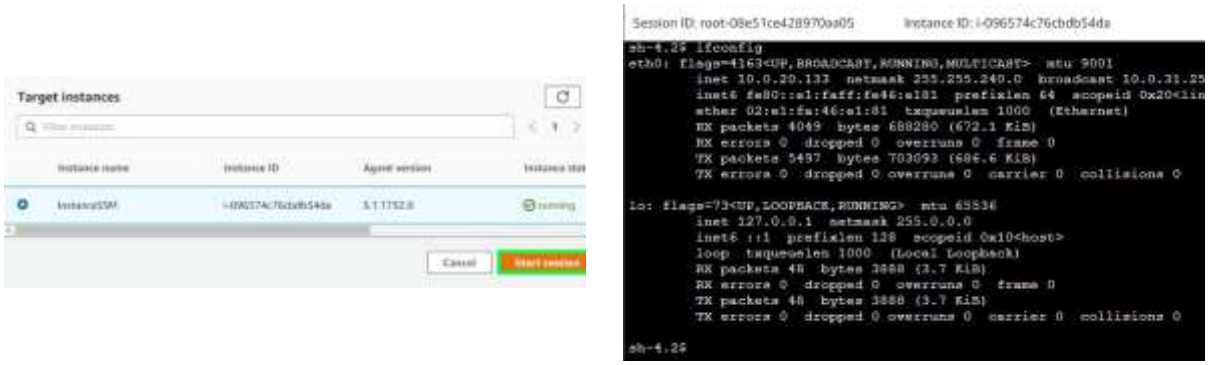
а) б)

Рисунок 15 – Консоль AWS Systems Manager: а) – Session Manager; б) – активація процедури з'єднання

Для з'єднання потрібно обрати віртуальний сервер, з яким здійснюватиметься з'єднання та активувати з'єднання кнопкою Start session (рис. 16а). Після активації відкривається нова вкладка і здійснюється з'єднання в браузері. Можна здійснити конфігурацію IP адреси для перевірки з'єднання з потрібним віртуальним сервером (рис. 16б). Параметри з'єднання можуть бути перевірені на вкладці details обраного віртуального сервера, зокрема можна перевірити приватну IP адресу.

Висновки

AWS пропонує два способи з'єднання з віртуальним сервером, що розташований в приватній підмережі. З'єднання через Bastion Host є найбільш розповсюдженим способом. Проте такий метод має ряд недоліків, як то запуск додаткового сервера та необхідність його адміністрування, ретельне налаштування мережі, а також необхідність адміністрування приватних ключів.



а) б)

Рисунок 16 – З’єднання з віртуальним сервером, що розміщений в приватній підмережі: а) – активація з’єднання; б) – власне з’єднання

Спосіб з’єднання за допомогою AWS Systems Manager позбавлений цих недоліків і є надзвичайно зручним для зареєстрованих користувачів. При цьому для шифрування трафіку використовуються протоколи TLS 1.2 та Sigv4.

Список літератури

[1] І. В. Кравченко, В. І. Микитенко, *Інформаційні технології*. Київ, КПІ ім. Ігоря Сікорського, 447 с., 2022.

[2] Офіційний сайт AWS. *Amazon Virtual Private Cloud (Amazon VPC)*. [Електронний ресурс]. Режим доступу : https://aws.amazon.com/vpc/

[3]] John R. Vacca, *Computer and Information Security Handbook* [3d ed.]. Cambridge, United States, 2017.

[4] П. Ю. Паталашко, Н. І. Кушніренко, “Автоматизація конфігурації безпечного під’єднання до корпоративних мереж”, *Інформатика та математичні методи в моделюванні*, Т. 12, №1-2, с. 73-83, 2022. doi: 10.15276/imms.v12.no1-2.73.

[5] Офіційний сайт IANA. *IANA IPv4 Special-Purpose Address Registry*. [Електронний ресурс]. Режим доступу : https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

[6] Офіційний сайт AWS. *Connect to the internet using an internet gateway*. [Електронний ресурс]. Режим доступу : https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

[7] Офіційний сайт AWS. *Configure route tables*. [Електронний ресурс]. Режим доступу : https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

[8] М. С. Мамута, І. О. Васильковська, І. В. Кравченко, О. Д. Мамута, “Дослідження способів з'єднання з віртуальним сервером AWS за мережевим протоколом Secure Shell” на *XII Міжнар. наук.-практ. конф. Modern Research in World Science*, Львів, 2023, с. 297-301

[9] Офіційний сайт AWS. *Set up to connect to your instance*. [Електронний ресурс]. Режим доступу : https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/connection-prereqs.html

[10] *Vi Editor with Commands*. [Електронний ресурс]. Режим доступу : https://www.javatpoint.com/vi-editor

[11] Офіційний сайт AWS. *AWS Systems Manager*. [Електронний ресурс]. Режим доступу : https://aws.amazon.com/systems-manager/

[12] Офіційний сайт AWS. *Working with SSM Agent*. [Електронний ресурс]. Режим доступу : https://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-agent.html

[13] Офіційний сайт AWS. *AWS Systems Manager Session Manager*. [Електронний ресурс]. Режим доступу : https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html

[14] Офіційний сайт AWS. *Step 2. Create VPC endpoints.* [Електронний ресурс]. Режим доступу : https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-create-vpc.html#sysman-setting-up-vpc-create

[15] Офіційний сайт AWS. *AWS Identity and Access Management* (IAM). [Електронний ресурс]. Режим доступу : https://aws.amazon.com/iam/

Стаття надійшла: 19.04.2023

References

[1] I. V. Kravchenko, V.I. Mykytenko, *Information technologies: Textbook*. Kiev: Igor Sikorsky KPI, 447 p., 2022. [in Ukrainian]

[2] AWS. *Amazon Virtual Private Cloud (Amazon VPC)*. [Online]. Available: https://aws.amazon.com/vpc/
[3]] John R. Vacca, *Computer and Information Security Handbook* [3d ed.]. Cambridge, United States, 2017.
[4] P. Patalashko, N. Kushnirenko, "Automation of Configurating Secure Connection to Corporate Networks", *Informatics and Mathematical Methods in Simulation*, Vol. 12, №1-2, pp. 73-83, 2022. DOI: https://doi.org/10.15276/imms.v12.no1-2.73. [in Ukrainian]
[5] IANA. *IANA IPv4 Special-Purpose Address Registry*. [Online]. Available : https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml
[6] AWS. *Connect to the internet using an internet gateway*. [Online]. Available : https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html
[7] AWS. *Configure route tables*. [Online]. Available : https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html
[8] M. Mamuta, I. Vasylkovska, I. Kravchenko, O. Mamuta, "Methods of Connection to AWS Virtual Server Using the Secure Shell Network Protocol" in *XII International conference. Modern Research in World Science*, Lviv, 2023, pp. 297-301. [in Ukrainian]
[9] AWS. *Set up to connect to your instance*. [Online]. Available : https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/connection-prereqs.html
[10] *Vi Editor with Commands*. [Online]. Available: https://www.javatpoint.com/vi-editor
[11] AWS. *AWS Systems Manager*. [Online]. Available: https://aws.amazon.com/systems-manager/
[12] AWS. *Working with SSM Agent*. [Online]. Available : https://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-agent.html
[13] AWS. *AWS Systems Manager Session Manager*. [Online]. Available : https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html
[14] AWS. *Step 2. Create VPC endpoints.* [Online]. Available : https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-create-vpc.html#sysman-setting-up-vpc-create
[15] AWS. *AWS Identity and Access Management* (IAM). [Online]. Available: https://aws.amazon.com/iam/

Відомості про авторів

Мамута Марина Сергіївна – к.т.н., старший викладач кафедри комп'ютерно-інтегрованих оптичних та навігаційних систем.

Кравченко Ігор Володимирович – старший викладач кафедри комп'ютерно-інтегрованих оптичних та навігаційних систем.

Мамута Олександр Дмитрович – к.т.н., науковий співробітник відділу когерентної і квантової оптики.

M. S. Mamuta, I. V. Kravchenko, O. D. Mamuta

METHODS OF CONNECTION TO AWS VIRTUAL SERVER LOCATED IN A PRIVATE SUBNET

National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kiev

Institute of Physics, National Academy of Sciences of Ukraine, Kiev